see p4

Software Design Specification

Oximax Project, Signature Verification Program

Monday, May 17, 1999~~Thursday, May 06, 1999~~

date of this draft

1 Overview

1.1 Purpose

This document describes the design of software to implement the services in the Software Requirements Specification for the Oximax signature project. The Oximax signature software will be developed as a set of software module to be used on the manufacturing line for sensors, and in the embedded firmware in pulse oximeters that interface to Oximax sensors.

2 Referenced Documents

SDS2 The Uptronics Software Development Plan will govern the development process. This is a change-controlled document, drawing number 060479.

The Statement of Work (SOW) dated February 11, 1999 sets forth the work to be accomplished.

The Specification, Product Requirement Document, Nellcor, indicates the product requirements. This is a change-controlled document, drawing number 0XXXXX.

The Software Requirements Specification presents High level Software Requirements derived from PRD. This is a change-controlled document.

SDS1 All C code written for the project shall conform to the Pleasanton Coding Standards, NP060307.

The strategy to protect oximeter sensor data was developed by Nellcor and Anagram Labs, as described in,

- Memo from Mike Fein, Protection plans for Digical oximeters and sensor, 03 Aug 1998.
- Memo from Thomas Berson, of 22 Oct 1998.

The project employs Rabin-Williams signatures, constructed in accordance with ISO/EIC 9796-2 of 1977.

We employ the SHA-1 hash function, defined in FIPS 180-1.

Technical references in this document refer to,

- *Handbook of Applied Cryptography,* by Alfred J, Menezes, Paul C. van Oorschot and Scott A. Vanstone, CRC Press 1997.

Key Management is now in a separate document, *Design of Key Management.*

3 Architecture

The signature system has three major functions:

EXHIBIT

C